

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-332019

(43)Date of publication of application : 30.11.2001

(51)Int.Cl.

G11B 20/10

(21)Application number : 2000-144456

(71)Applicant : TAIYO YUDEN CO LTD

(22)Date of filing : 17.05.2000

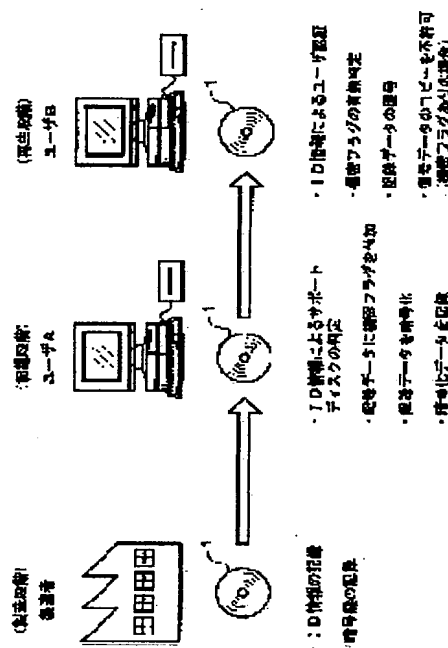
(72)Inventor : OMURA YUKIHIDE
SUNAKAWA RYUICHI
SHIMIZU HIRONOBU

(54) DATA RECORDING AND REPRODUCING METHOD FOR WRITE-ONCE TYPE OPTICAL DISK, DATA REPRODUCING DEVICE FOR WRITE-ONCE TYPE OPTICAL DISK AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data recording and reproducing technique for a write-once type optical disk which can surely prohibit the reutilization of plaintext data after decoding without expecting the morality on a reproducing side user and can therefore assure the security in all stages from recording to reproducing.

SOLUTION: In writing data to the write-once type optical disk, the data is written by adding a prescribed confidential flag to the data and when the writing data is reproduced, the presence or absence of the confidential flag is inspected. When the presence of the confidential flag is detected, the operation relating to the formation of the copy of the data is restricted. The reutilization of the reproduced data may be obstructed and the security in the reproduction stage assured.



LEGAL STATUS

[Date of request for examination]

02.10.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-332019
(P2001-332019A)

(43) 公開日 平成13年11月30日 (2001. 11. 30)

(51) Int. Cl.⁷
G 1 1 B 20/10

識別記号

F I
G 1 1 B 20/10フォーマット (参考)
H 5 D 0 4 4

審査請求 未請求 請求項の数 4 O L (全 20 頁)

(21) 出願番号 特願2000-144456 (P2000-144456)

(22) 出願日 平成12年5月17日 (2000. 5. 17)

(71) 出願人 000204284

太陽誘電株式会社
東京都台東区上野6丁目16番20号

(72) 発明者 大村 幸秀

東京都台東区上野6丁目16番20号 太陽誘
電株式会社内

(72) 発明者 砂川 隆一

東京都台東区上野6丁目16番20号 太陽誘
電株式会社内

(74) 代理人 100096899

弁理士 鹿嶋 英實

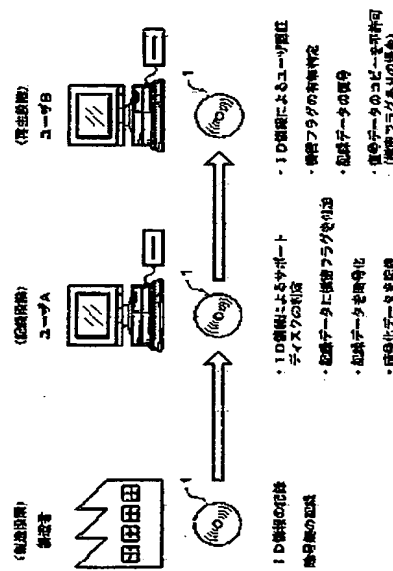
最終頁に続く

(54) 【発明の名称】 ライトワンス型光ディスク用データ記録再生方法、ライトワンス型光ディスク用データ再生装置
および記録媒体

(57) 【要約】

【課題】 再生側ユーザのモラルに期待することなく復号後の平文データの再利用を確実に禁止し、以って、記録から再生までのあらゆる段階のセキュリティを確保できるライトワンス型光ディスク用データ記録再生技術を提供する。

【解決手段】 ライトワンス型光ディスクにデータを書き込む際に所定の機密フラグを前記データに付加して書き込み、前記書き込みデータを再生する際に前記機密フラグの有無を検査して機密フラグの存在が検出された場合に前記データの複製物の生成に関する動作を制限する。再生データの再利用を阻止し、再生段階におけるセキュリティを確保できる。



(2)

特開2001-332019

1

【特許請求の範囲】

【請求項1】 ライトワンス型光ディスクにデータを書き込む際に所定の機密フラグを前記データに付加して書き込む書き込み工程と、
前記書き込みデータを再生する際に前記機密フラグの有無を検査して機密フラグの存在が検出された場合に前記データの複製物の生成に関する動作を制限する複製制限工程と、
を含むことを特徴とするライトワンス型光ディスク用データ記録再生方法。

【請求項2】 前記光ディスクのシステム領域に格納されたセキュリティ情報に基づき該光ディスクへのアクセスを制限するアクセス制限工程をさらに具備することを特徴とする請求項1記載のライトワンス型光ディスク用データ記録再生方法。

【請求項3】 ライトワンス型光ディスクから読み込まれたデータの中に所定の機密フラグが含まれているかを判定する判定手段と、

該判定手段によって機密フラグの存在が判定された場合に前記データの複製物の生成に関する動作を禁止する禁止手段と、

を備えたことを特徴とするライトワンス型光ディスク用データ再生装置。

【請求項4】 ライトワンス型光ディスクから読み込まれたデータの中に所定の機密フラグが含まれているかを判定する判定手段と、

該判定手段によって機密フラグの存在が判定された場合に前記データの複製物の生成に関する動作を禁止する禁止手段と、

を実現するためのプログラムを格納したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ライトワンス型光ディスク用データ記録再生方法、データ再生装置および記録媒体に関する。詳しくは、1回だけデータを書き込むことができるCD-R (Compact Disc Recordable) に代表されるライトワンス型光ディスクに適用するデータ記録再生方法、データ再生装置および記録媒体に関する。

【0002】

【従来の技術】 各種コンテンツやコンピュータプログラム等の電子データの配布媒体に、CD-ROM (Compact Disc Read Only Memory) が多用されている。CD-ROMは、電子データを記録したマスタCDからプレス成型等によって製造される複製物であり、主に大量配布のメディアに用いられるが、配布数（製造数）の少ないサンプル版CDやプライベートCDなどには、データの消去や書き込みができない（追記は可能）ライトワンス型の光ディスク装置、典型的にはCD-Rが用いられる。

2

CD-Rは透明なディスク基板と反射層（詳細な構造は後述する。）との間に有機色素からなる記録層を有している点でCD-ROMと構造上の違いがあり、専用の記録装置（CD-Rライター）を用いて当該記録層に高出力レーザを照射し、熱的反応によって当該記録層に情報ビットを形成することにより、ユーザ段階で情報の記録を行うことができるものである。

【0003】 CD-Rは、上記のとおりデータの消去や書き込みができないライトワンス型の記録媒体である。すなわち、一度書き込んだデータの消去や書き換えが不可能である。そのため、不正者によるデータの消去や改ざんを確実に防止できるという優れた利点を待つことから、今日、特に秘匿を要する電子データの保管や配布などの用途に欠かせない記録媒体としての地位を確立しているが、反面、CD-Rは記録情報の読み出しが自由であるが故に、情報の不正読み出しや不正コピーを防止できないという欠点も持っている。

【0004】 そこで、秘匿を要するデータを記録する際に、例えば、図16に示すように、暗号化して記録することが行われている。図において、平文データ100は暗号化前の「生」のデータであり、例えば、可読性を有するテキスト形式のデータである。この平文データ100を不可視化して記録する場合、まず、所定の暗号化ツール101を用いて暗号化データ102に変換する。暗号化の方式は特に限定しないが、暗号鍵と復号鍵に共通の鍵を用いる共通鍵方式である。以下、この鍵のことを代表して「暗号鍵」ということにする。したがって、以下において、暗号鍵という場合は復号鍵も意味することとする。

【0005】 さて、暗号化されたデータ（図においては暗号化データ102）は不可視データであり、そのまま配布しても安全（計算量的に安全）であるため、この暗号化データ102をCD-R103に書き込むことによってデータの不正読み取りを防止し、セキュリティを保つことができる。再生の際は、CD-R103から暗号化データ104を読み出し、所定の復号ツール105を用いて平文データ106に戻せば（復号すれば）よい。

【0006】

【発明が解決しようとする課題】 しかしながら、上記のセキュリティ対策にあつては、復号後のデータ（平文データ106）の再利用が自由であり、データ保全の効果はもっぱらCD-R103に収められた状態でしか得られないという不都合がある。すなわち、CD-R103から読み出されて復号された後の平文データ106については、まったくセキュリティがかかっておらず、この平文データ106に対するデータ保全は単に再生側ユーザのモラルに期待するしかないという問題点があった。

【0007】 したがって、本発明が解決しようとする課題は、再生側ユーザのモラルに期待することなく復号後の平文データの再利用を確実に禁止し、以て、記録か

(3)

特開2001-332019

3

ら再生までのあらゆる段階のセキュリティを確保できる
ライトワンス型光ディスク用データ記録再生技術を提供
することにある。

【0008】

【課題を解決するための手段】請求項1記載のライトワ
ンス型光ディスク用データ記録再生方法は、ライトワ
ンス型光ディスクにデータを書き込む際に所定の機密フラ
グを前記データに付加して書き込む書き込み工程と、前
記書き込みデータを再生する際に前記機密フラグの有無
を検査して機密フラグの存在が検出された場合に前記デ
ータの複製物の生成に関する動作を制限する複製制限工
程と、を含むことを特徴とする。これによれば、データ
の再生時に所定の機密フラグが検出されると、再生デー
タの複製物の生成が制限される。請求項2記載のライト
ワンス型光ディスク用データ記録再生方法は、請求項1
記載のライトワンス型光ディスク用データ記録再生方法
において、前記光ディスクのシステム領域に格納された
セキュリティ情報に基づき該光ディスクへのアクセスを
制限するアクセス制限工程をさらに具備することを特徴
とする。これによれば、光ディスクのシステム領域に不
可視状態で格納されたセキュリティ情報に基づいて光デ
ィスクへのアクセスが制限される。請求項3記載のライ
トワンス型光ディスク用データ再生装置は、ライトワ
ンス型光ディスクから読み込まれたデータの中に所定の機
密フラグが含まれているか否かを判定する判定手段と、
該判定手段によって機密フラグの存在が判定された場合
に前記データの複製物の生成に関する動作を禁止する禁
止手段と、を備えたことを特徴とする。これによれば、
データの再生時に所定の機密フラグが検出されると、再
生データの複製物の生成が禁止される。請求項4記載の
記録媒体は、ライトワンス型光ディスクから読み込ま
れたデータの中に所定の機密フラグが含まれているか否
かを判定する判定手段と、該判定手段によって機密フラ
グの存在が判定された場合に前記データの複製物の生成
に関する動作を禁止する禁止手段と、を実現するためのプ
ログラムを格納したことを特徴とする。これによれば、
マイクロコンピュータを含むハードウェアリソースと該
プログラムとの有機的結合によって前記判定手段および
禁止手段が実現される。

【0009】

【発明の実施の形態】以下、図面を参照して本発明の実
施の形態を詳細に説明する。なお、以下の説明における
様々な細部の特定ないし実例および数値や文字列その他
の記号の例示は、本発明の思想を明瞭にするための、あ
くまでも参考であって、それらのすべてまたは一部によ
って本発明の思想が限定されないことは明らかである。
また、周知の手法、周知の手順、周知のアーキテクチャ
および周知の回路構成等（以下「周知事項」）については
その細部にわたる説明を避けるが、これも説明を簡潔
にするためであって、これら周知事項のすべてまたは一

4

部を意図的に排除するものではない。かかる周知事項は
本発明の出願時点で当業者の知り得るところであるの
で、以下の説明に当然含まれている。

【0010】まず、本実施形態のライトワンス型光ディ
スク（以下「CD-R」という。）の利用形態を大まか
に説明する。図1は、本実施形態のCD-R1の利用模
式図である。この図では、製造者（メーカー）によるCD
-R1の製造段階、ユーザAによる当該CD-R1への
秘匿を要するデータの記録段階、および、ユーザBによ
る当該記録済みCD-R1からデータを読み出して再生
する再生段階の三つの段階が示されている。

【0011】後の説明からも明らかになるが、（1）製
造段階ではCD-R1に固有の識別情報（以下「ID情
報」という。）と所定の暗号化方式における暗号鍵（復
号鍵を兼ねるもの）とをCD-R1に電子的に記録して
出荷する。ID情報と暗号鍵の記録場所はユーザからの
直接的なアクセスが許可されていない場所（システム領
域；領域構造については後述する。）である。（2）記
録段階ではそのCD-R1のID情報から当該CD-R
1が所定の製造者またはあらかじめ登録された製造者
によって作られたもの（以下「サポートディスク」とい
う。）であるか否かを判定し、サポートディスクである
場合に、記録データに所定の「機密フラグ」を付加する
と共に、CD-R1に書き込まれている暗号鍵を用いて
記録データ（機密フラグを付加したもの）を暗号化し、
その暗号化データをCD-R1に記録する。（3）再生
段階ではCD-R1のID情報を用いてユーザ認証を行
い、正規ユーザ（ID情報を知っているユーザ）に対し
てのみ暗号化データの復号処理を許可すると共に、復号
データのコピーや保存等の複製処理を実行して再利用
を行う場合は、記録データ中の「機密フラグ」の有無を判
定し、機密フラグ有りの場合は上記再利用を拒否。例え
ば、コピー動作や保存動作を強制中断する。

【0012】これら三つの段階において、CD-R1に
セキュリティを持たせるための工夫は、①製造時にCD
-R1のシステム領域にID情報と暗号鍵を書き込むよ
うにしたこと、②ユーザAによる記録時に、記録データ
に「機密フラグ」を付加するようにしたこと、③同記録
時に記録データ（機密フラグ付）を暗号化してCD-R
1に書き込むようにしたこと、④ユーザBによる再生時
にID情報によるユーザ認証を行って正規ユーザに対し
てのみ暗号化データの復号を許可するようにしたこと、
⑤同再生時に復号データの再利用が行われる場合は機密
フラグの有無を判定して機密フラグ有りの場合にその再
利用動作を強制中断するようにしたことにある。

【0013】①のID情報はデータ再生時のユーザ認証
に用いられ、また、①の暗号鍵はデータの暗号化と正規
ユーザによって行われる暗号化データの復号に用いられ
る。これらのID情報と暗号鍵はCD-R1の記録領域
のうちユーザアクセスが許可されていない領域（システ

(4)

特開2001-332019

5

ム領域)に書き込まれた、いわば不可視化された“隠しデータ”である。①のID情報はまたデータ書き込み時におけるサポートディスクの判定にも用いられる。サポートディスクとは、前記のとおり、所定の製造者またはあらかじめ登録された製造者によって作られたCD-R1のことであり、正確には“機密フラグ”を用いて行われる復号後データの再利用禁止対策を“サポート”した特別なディスク(CD-R1)であることを意味する。

【0014】ここで、機密フラグはその名前のとおりフラグ形式のデータであってもよいし、フラグ以外の別形式であってもよい。留意すべき点は機密フラグ(または機密フラグと同等のもの)の存在がユーザに対して秘匿化されていなければならないことにある。一般にフラグ形式のデータは二値論理(ブーリアン型ともいう。)の1ビットデータであり、そのビット位置を非公開とすることによって一応の秘匿化は可能であるが、終当りて調べられた場合にフラグの位置が見破られるおそれを否定できないため、望ましくは、電子透かしのような積極的な秘匿化対策を講じたデータとすることが好ましい。電子透かしとは、オリジナルデータの品質を損なうことなく、そのオリジナルデータの周波数、空間または時間の一つまたは複数のドメインに所定のメッセージ情報を隠す(埋め込む)ことをいう。機密フラグは、再生段階において、復号後の平文データの再利用(平文データを他の記録媒体にコピーや保存したりすること;複製動作ともいう。)を禁止するためのチェックフラグとして用いられる。これにより、暗号化データによるCD-R1のセキュリティに加え、復号後の平文データのセキュリティ対策も講じることができ、本願発明の課題である、再生側ユーザのモラルに依存することなく復号後の平文データの再利用を禁止でき、以って、記録から再生までのあらゆる段階のセキュリティを確保できるライトワンス型光ディスクを提供することができるのである。

【0015】以下、上記課題達成に必要な構成および作用について、具体例をあげて説明する。図2は、本実施形態におけるCD-R1の外観図(a)およびその要部拡大図(b)である。これらの図において、CD-R1は、直径12cm(直径8cmのものもある。以下、直径12cmのもので説明する。)のディスク状を有しており、ディスクの中心に直径15mmのセンターホール1aが形成されている。ディスクの中心T0からセンターホール1aの壁(ディスク内縁T1)までの距離は7.5mm、T0からディスク外縁T7までの距離は60mmであり、このT1~T7の間に同心状の複数の記録領域、すなわち、ディスクの内周側から順にPCA(Power Calibration Area)、PMA(Program Memory Area)、リードイン(図では「RI」と略している。)、データエリア(図では「UA」と略している。)およびリードアウト(図では「RO」と略している。)の各領域が設けられている。

6

【0016】各領域を概説すると、T2~T3に位置するPCAは、CD-R1にデータを記録する際に行われるレーザ強度調整のための試し書き領域である。この試し書きは一般に100回程度可能であり、少なくとも1回のデータ記録で1回分の領域を消費する。T3~T4に位置するPMAは、CD-R1でまだクローズしていないセッションのトラックがあるとき、そのトラック番号と開始/終了位置を一時的に保存する領域である。T4~T5に位置するリードイン(RI)は、セッショントラックの先頭(ディスクの内周側)にある領域で、セッションのTOC(Table Of Contents: CDに記録されているトラック数、開始位置およびデータ領域の合計の長さ)を保存する領域である。セッションをクローズすると、PMAに一時保存されていた情報がこのリードイン(RI)に書き込まれる。

【0017】T5~T6に位置するデータエリア(UA)は、ユーザ段階で実際にデータが書き込まれる領域である。データの記録容量は最大約680Mバイト(直径8cmのものは最大約190Mバイト)であり、この記憶容量は録音時間で表すと最大約74分(直径8cmのものは最大約21分)になる。データエリア(UA)は、リードイン(RI)のすぐ後ろから連続する所定サイズ(2Kバイト)単位の論理ブロックで管理されるようになっており、各論理ブロックごとに0から最大約330000までのLBN(Logical Block Number)が割り当てられるようになっている。T6~T7に位置するリードアウト(RO)は、セッションの最後(ディスクの外周側)にある領域で、データエリア(UA)の最後に到達したことを示す領域である。

【0018】これら各領域のディスク上の位置はT3を除いて規格化されている。すなわち、T2はT0から22.5mm離れた位置、T4はT0から23mm離れた位置、T5はT0から25mm離れた位置、T6はT0から58mm離れた位置となるように規定されている。なお、図ではディスク外縁とリードアウト(RO)の終了位置とを同一の符号(T7)で示しているが、これは図示の都合である。リードアウト(RO)の実際の終了位置はT0から58.5mm離れた位置になる。以下、特に断りのない限り、T7はリードアウト(RO)の終了位置を表すものとする。ちなみに、リードアウト(RO)の開始と終了位置(T6およびT7)はCD-R1に記録するデータの量に応じて変化する。上記の実際値(T6=58mm、T7=58.5mm)は記憶データ量を最大にしたときのものである。

【0019】図3は、CD-R1の断面構造図である。CD-R1は、透明で耐熱性、耐湿性および成形性に優れ、且つ、所要の光学的特性(屈折率や複屈折など)を備えた材料(例えばプラスチック)からなる基板1bの上に、有機色素からなる記録層1c、アルミニウムなどの金属材料からなる反射層1dおよび樹脂等の硬質材料

(5)

特開2001-332019

7

からなる保護層1eを積層して形成されている。断面全体の厚さは1.2mmである。

【0020】CD-ROMとの構造上の相違は、記録層1cを有する点、および記録層1cと基板1bとの間にウォッブルグループと呼ばれる渦巻状の案内溝1fが形成されている点にある。CD-R1へのデータの記録は基板1bの裏側から案内溝1fに沿って記録用の強いレーザを照射し、記録層1cを加熱して情報ビット(Pit:再生用のレーザ反射光を変調するための物理的変形変質部分)を形成することにより行われる。案内溝1fは、ディスクの内周側から外周側(または外周側から内周側)に向かって一筆書きの要領で連続して形成されており、案内溝1fの幅は約0.5~0.7μm、間隔は約1.6μmである。ユーザ段階におけるデータ記録は、案内溝1fに沿って、その案内溝1f(または案内溝1fの間のランド部)直下の記録層1cに情報ビットを形成することによって行われる。なお、CD-R1の裏側から見て案内溝1fの凸部分をランド(山)、凹部分をグループ(谷)といい、一般に谷の部分にウォッブルグループというが、本明細書では山と谷を区別しない。

【0021】ここで、案内溝1fの一の役割は、ユーザ段階のデータ記録時にディスクの回転速度を制御するためのタイミング情報を保持することにある。この役割のため、案内溝1fは、所定の周期(例えば22.05kHzに相当する周期)で蛇行(「ウォブリング」ともいう。)する形状に形成されている。データの記録時には、この蛇行を光ピックアップでトレースして周期を検出し、その検出周期が一定となるようにディスクの回転速度を制御することにより、データ記録時の光ピックアップとディスク間の相対速度を一定に保つ。案内溝1fの他の役割は、ディスク上の各記録領域(PCA、PMA、RI、UAおよびRO)の位置情報をはじめとした様々なディスク情報を保持することにある。ディスク情報はATIP(Absolute Time In Pregroove:通称「Aチップ」という。)とも呼ばれており、ATIPには、上記の位置情報のほかに、基準の記録レーザ強度やディスク回転速度、アプリケーションコードあるいはディスクタイプなどの各種情報が含まれている。

【0022】図4は、CD-R1の各記録領域のフォーマット概念図である。この図において、PCA、PMA、リードイン(RI)、データエリア(UA)およびリードアウト(RO)はそれぞれ、図2(b)における同名部分に対応する。PCAおよびPMAのサイズ(情報書き込み可能容量)は特に決められていないが、前述の試し書き回数(一般に100回程度)やセッション情報の一時記憶回数に見合った必要量、例えば、PCAで約3.5Mバイト程度、PMAで約2Mバイト程度の容量が確保されている。ちなみに、これらの例示容量からPCAの開始位置(T2)とPMAの開始位置(T3)

8

は、規格化されたリードイン(RI)の開始位置(T4)を基準として、「T2=T4-約3.5秒」の位置、「T3=T4-約1.3秒」の位置と書き表すことができる。

【0023】既述のとおり、PCAはデータ記録を行う際の試し書き領域、PMAはクローズされていないセッション情報を一時的に格納する領域であるから、これら二つの領域(PCA/PMA)はデータ記録時のみ利用(アクセス)される領域である。一方、リードイン(RI)はクローズされたセッション情報をTOCとして記録する領域、データエリア(UA)は実際にデータが書き込まれる領域、リードアウト(RO)はデータエリアの終わりを明示する領域であるから、これら三つの領域(リードイン/データエリア/リードアウト)はデータ記録時と再生時の両方で利用(アクセス)される領域である。

【0024】他方、これらすべての領域をユーザからのアクセス容易性の点で見ると、すなわち、CD-R1の読み取り装置を備えたパーソナルコンピュータ等の利用者からその記憶内容を通常のツール(典型的には当該パーソナルコンピュータに搭載されたオペレーティングシステム上のファイルシステムなど)を用いて容易にアクセスできるか否かの点で評価すると、データエリア(UA)については当然ながらその記憶内容の全容把握は可能であるが、他の領域(PCA、PMA、リードインおよびリードアウト)の内容把握は不可能である。

【0025】もちろん、特殊なツールを使用すれば可能ではあるが、そのようなツールは一般のユーザにとって入手困難であるため、かかる例外的なツールの利用を除けば、データエリア以外の他の領域(PCA、PMA、リードインおよびリードアウト)は、システムからのアクセスだけが許可された特殊な領域であるといえることができる。本明細書では、この特殊領域のことを「システム領域」といい、ユーザからのアクセスが許可された領域のことを「ユーザ領域」という。すなわち、データエリア(UA)はユーザ領域、それ以外のPCA、PMA、リードイン(RI)およびリードアウト(RO)はシステム領域である。

【0026】本実施の形態におけるCD-R1は、先に説明したとおり、製造段階でシステム領域の一部にCD-R1の固有情報(以下「ID情報」という。)と所定の暗号鍵情報とが書き込まれる。ID情報はCD-R1の全製造数にわたってユニークな値(重複しない値)を持つことが望ましいが、製造数が膨大になる場合、情報ビットが多ビット化してシステム領域の記憶容量を圧迫する懸念があるため、例えば、製造ロットごとや製造ラインごとまたは製造時期ごとに異なる情報としてもよい。

【0027】このID情報は、後述するように、ユーザ段階でのCD-R1へのアクセス照合に用いられる。例

(6)

特開2001-332019

9

えば、データの再生を行うアプリケーションでIDの入力を要求し、入力されたIDとシステム領域に書き込まれているIDとの一致を判定して、一致の場合のみアクセスを許可する。これにより、不正なユーザ（IDを知らないユーザ）によるデータの再生や複製を阻止し、データの流出や不正生成物の出現を回避することができる。

【0028】CD-R1に書き込まれたID情報のユーザへの通知は、各々のCD-R1の購入者（または正規入手者）ごとに行わなければならない。例えば、あるCD-R1（以下、便宜的に「ディスクA」とする。）に書き込まれたID情報を“abcdef”と仮定すると、ディスクAの購入者または正規入手者に対し、当該ID情報（“abcdef”）を書面ないしその他の手段で通知する。この手段としては、例えば、ディスクAのパッケージ（ディスクAを収めたプラスチックケース）の中に当該ID情報（“abcdef”）を記載した紙片を入れておいてもよいし、ディスクAの購入時等に口頭で伝えてもよい。その他いろいろな手段が考えられるが、要は、出荷時にCD-R1に書き込んだID情報をユーザに正確に伝達できればよい。

【0029】一方、製造段階でシステム領域に一緒に書き込まれる鍵情報は、ユーザ段階でデータエリアに書き込まれる生データを暗号化するために用いられる。すなわち、データの記録を行うアプリケーションで暗号鍵を読み出し、この暗号鍵を用いて生データを暗号化データに変換した後、その暗号化データをCD-R1のデータエリアに書き込む。この暗号鍵は暗号化データを復号する際にも用いられる。すなわち、データの再生時に、データの再生を行うアプリケーションでIDの入力を要求し、入力されたIDとシステム領域に書き込まれているIDとの一致を判定して、一致の場合に暗号鍵と暗号化データを読み出し、その暗号鍵を用いて暗号化データを復号し、生データに変換してユーザの利用に供する。

【0030】したがって、IDを知らない不正なユーザは、データへのアクセス自体を拒否されるから、不正なデータの読み取りを回避できると共に、万が一、何らかの手段でアクセスが成功したとしても、システム領域に書き込まれた暗号鍵へのアクセスは通常の技術知識では不可能であるから、暗号化データを生データに復号することができず、この点において万全の保全策を講じることができる。

【0031】図5は、システム領域に書き込まれるID情報と暗号鍵を含むデータフォーマットの例示構成図である。この図において、第一の例（a）は、8バイトのID情報、8バイトのDES（Data Encryption Standard：アメリカ連邦政府標準暗号規格）暗号鍵、2バイトの製造年、1バイトの製造月および1バイトの製造日の各情報から構成された全部で20バイトの大きさを有している。また、第二の例（b）は、8バイトのID情報、24バイトのトリプルDES暗号鍵、2バイトの製造年、1バイトの製造月および1バイトの製造日の各情報から構成された全部で36バイトの大きさを有している。いずれのフォーマットを採用するかは、もっぱら暗号鍵の信頼性を重視するか、または、システム領域の記憶容量圧迫を回避するかで決まる。なお、図示のバイト数や暗号鍵の種類およびフォーマット構成はあくまでも例示である。要はCD-R1の固体識別が可能な情報（ID情報）と、生データを暗号化データに変換できる共に暗号化データから生データに復号できる所定のキー情報（暗号鍵）とをCD-R1のシステム領域に書き込んでおけばよい。

10

【0032】図6は、ライトワンス型光ディスク記録再生装置（以下「CD-R記録再生装置」という。）の概略的なブロック構成図である。このCD-R記録再生装置10は、CD-R1のクランピングエリア（図2（a）のT1～T2の間に設けられた情報非記録エリア）を担持して所定方向に回転駆動するスピンドルモータ12と、CD-R1の基板1bを透過して記録層1cに記録用または再生用のレーザ（一般に波長770～830nmの赤外レーザ）13を照射する光ピックアップ14と、光ピックアップ14の内部に設けられた不図示のシークモータと協調して光ピックアップ14をディスクの半径方向に移動させる粗動モータ15とを備えると共に、スピンドルモータ12の回転速度を制御するディスク回転制御部16と、粗動モータ15の回転速度と回転方向を制御する粗動モータ制御部17と、光ピックアップ14の位置やレーザ強度の制御を行うピックアップ制御部18と、光ピックアップ14からの読み取り信号や光ピックアップ14への書き込み信号の波形変換等の制御を行う再生/記録制御部19とを備え、さらに、これらの各制御部を統括するコントローラ20を備える。

【0033】CD-R記録再生装置10は、パーソナルコンピュータ等のホスト装置21の拡張スロットに内蔵され（または外付けされ）、ホスト装置21とコントローラ20との間を所定の信号規格（例えば、SCSI：Small Computer System Interface）のケーブル21aで接続して用いられる。

【0034】このような構成を有するCD-R記録再生装置10は、以下に示すとおり、CD-R1への情報の記録とその記録情報の再生を行うことができる。なお、CD-R1はCD-ROMコンパチのデバイスであり、CD-R記録再生装置10は、CD-ROMの情報再生も可能であるが、本発明とは直接の関連がないため説明を省略する。

【0035】＜CD-R1への情報の記録動作＞ホスト装置21でCD-R記録専用アプリケーションプログラム（以下「ライティングプログラム」という。）を実行すると、まず、ライティングプログラムからのレーザ強度キャリブレーションコマンドがコントローラ20に伝

50

(7)

特開2001-332019

11

えられる。コントローラ20はこのコマンドに応じて各制御部に所定の指令を伝え、光ピックアップ14をCD-R1のPCA空領域(試し書きされていない領域)に位置させると共に、スピンドルモータ12の回転速度を制御(光ピックアップ14の現在位置における相対速度が所定速度となるように制御)した後、光ピックアップ14から暫定強度(5.5~8mWの間の任意パワー)の記録用レーザ13をPCA空領域に照射して試し書きを行う。光ピックアップ14の位置制御およびスピンドルモータ12の回転速度制御は、CD-R1の案内溝11fのトレース信号から再生された情報(タイミング情報およびATIP情報)に従って行われる。

【0036】次いで、コントローラ20は、再生/記録制御部19を介してPCAに試し書きされたデータを読み取り、そのデータをホスト装置21のライティングプログラムに返送する。ライティングプログラムは、試し書きデータと期待値とを比較してレーザ強度の適否を判定し、判定結果が「否」であればレーザ強度を増減調節して再びレーザ強度キャリブレーションコマンドを発行する一方、判定結果が「適」であれば、CD-R1への情報の記録動作を開始する。

【0037】この記録動作は、ユーザによって適宜に選択された所要の記録データをライティングプログラムからコントローラ20に伝え、このコントローラ20の制御の下、各制御部を介してスピンドルモータ12の回転制御および光ピックアップ14の位置制御を行いつつ、上記記録データで光ピックアップ14からの記録用レーザ13を調節しながらCD-R1のデータエリアに記録を行っていくというものである。そして、記録を完了すると、すべてのセッションを閉じ、そのセッション情報のTOCをリードイン(RI)に書き込むと共に、最終セッションの後にリードアウト(RO)を形成する。

【0038】<CD-R1の記録情報の再生動作>CD-R1の記録情報を再生する際上記ライティングプログラムは不要である。但し、CD-R1のファイルシステムとホスト装置21のファイルシステムとの相互変換を行うためのドライバソフトの類は必須である。ユーザはこのドライバソフトを介してCD-R記録再生装置10を利用することにより、ホスト装置21に装備されたハードディスク等の他の記憶デバイスとの区別を意識せずにCD-R1のファイルシステムにアクセスすることができる。すなわち、ユーザにはオペレーティングシステムのファイルシステムによって認識されたファイル構造が見えるから、ユーザは、他の記憶デバイスに格納されたファイルと同様の手順でCD-R1内の目的とするファイルを利用することができるようになっていく。

【0039】CD-R記録再生装置10は、このファイルアクセスに際して、リードイン(RI)内のTOC情報を読み出してホスト装置21のドライバソフトに提供すると共に、当該ドライバソフトから特定ファイルの読

12

み出しコマンドを受け取った場合は、リードイン(RI)内のTOC情報を参照して当該ファイルのデータが書き込まれたデータエリア(UA)のトラックを特定し、そのトラックの開始位置に光ピックアップ14を位置させると共に、スピンドルモータ12の回転速度を制御し、光ピックアップ14から再生用のレーザ(パワーが0.2mW程度に抑えられる点を除き記録用のレーザと同じもの)13をCD-R1に照射して当該ファイルデータを読み取り、その読み取りデータをホスト装置21に転送するという一連の動作を実行する。

【0040】このように、CD-R記録再生装置10は、CD-R1への情報の書き込みを行うことができると共に、CD-R1に書き込まれた情報の再生も行うことができる。このCD-R記録再生装置10は、記録段階でCD-R1への情報の書き込みを行う場合に必要不可欠な構成要素であるが、再生段階で、CD-R1に書き込まれた情報の再生を行う場合にも必要とされる構成要素である。CD-R1はCD-ROMコンパチのデバイスで、昨今のパーソナルコンピュータ等のほとんどにはCD-ROM再生装置が搭載されており、そのCD-ROM再生装置を利用してCD-R1の情報の再生を行うことも可能であるが、このCD-ROM再生装置は、CD-R1のシステム領域に書き込まれたID情報や暗号鍵にアクセスできないから、やはり、CD-R1に書き込まれた情報の再生を行う場合もCD-R記録再生装置10は欠かせない構成要素である。

【0041】また、CD-R記録再生装置10はもっぱらユーザによる記録や再生で使用される装置であるが、CD-R1への情報書き込み機能に注目すると、その基本的動作は、CD-R1の製造段階で行われるID情報や暗号鍵の書き込みにも適用可能であるから、以下の説明では上記のCD-R記録再生装置10をユーザ段階と製造段階の両方で使用されるものとして話を進める。

【0042】<出荷時情報記録処理>図7は、CD-R1の製造段階におけるID情報と暗号鍵の書き込み動作(以下「出荷時情報記録処理」という。)を示すフローチャートである。なお、製造段階では、CD-R記録再生装置10の記録機能しか利用しないため、図示のフローチャートではCD-R記録再生装置10のことを便宜的に「記録機」と称している。但し、この用語(記録機)には、CD-R記録再生装置10に限らず、製造段階専用の「記録機」であってもよい旨の意図も含まれている。

【0043】図において、出荷時情報記録処理を開始すると、まず、未記録のCD-R1(フロー中では「ディスク」と称する。)を用意し、このCD-R1を記録機に装填する(ステップS11)。次に、ホスト装置21を操作してCD-R1への記録情報を手入力または自動生成する(ステップS12)。この記録情報はCD-R1のID情報や所定の秘密鍵および当日の日付(作成日

(8)

特開2001-332019

13

付) などであり、そのフォーマットは、図5(a)または(b)に示すとおりである。

【0044】次いで、ホスト装置21から記録機に対して情報記録命令を発行すると(ステップS13)、記録機はこの命令に応答してレーザ強度キャリブレーション処理を実行し、適正なパワーに記録用レーザ13を設定した後、光ピックアップ14をCD-R1の記録領域の「特定位置」に移動制御する(ステップS14)。この特定位置は原理的にはユーザからの直接的なアクセスが認められていない領域、すなわち、システム領域(PC A、PMA、リードインまたはリードアウト)の未使用領域上の任意位置である。特に好ましくは、データ再生時にその存在が無視される領域として当業者に広く認知されているPCAまたはPMA上の(未使用領域上の)任意位置である。以下、説明の便宜上、上記「特定位置」をPCAの未使用領域上の任意位置とする。

【0045】次いで、記録機は、ホスト装置21から記録情報(ステップS12で生成した情報)を受け取り、その記録情報を用いて記録用レーザ13を調整しつつ、記録用レーザ13をCD-R1の透明な基板1bを介して記録層1cの案内溝1fに照射し、案内溝1f直下の記録層1cに情報ビットを形成して、前記記録情報のCD-R1への書き込みを行う(ステップS15)。記録情報の書き込み開始位置は、上記ステップS14で実行された光ピックアップ14の移動位置、すなわち、PCAの未使用領域上の任意位置であり、記録情報の書き込み終了位置は当該位置から記録情報のサイズ(例えば、図5のフォーマットに従えば20バイトまたは36バイト)に相当する分だけ離れた位置である。

【0046】次いで、記録機は、光ピックアップ14を上記特定位置に復帰させると共に、当該位置を再生開始位置、記録情報のサイズに相当する分だけ離れた位置を再生終了位置として、システム領域に書き込んだ記録情報の再生を行い、この再生情報をホスト装置21に転送する。ホスト装置21は、記録機から転送された再生データと上記記録情報とを比較照合してバリファイ検査を行い(ステップS16)、両者が一致していれば正常に書き込みを行えたと判断してその旨を作業者に報知する一方、そうでなければ書き込みを失敗したと判断してその旨を作業者に報知する(ステップS17)。作業者は、正常書き込み報知の場合に当該CD-R1を出荷棚へ移動し(ステップS18)、書き込み失敗報知の場合に当該CD-R1を不良品棚へ移動する(ステップS19)。そして、以上の処理を用意されたCD-R1がなくなるまで繰り返して実行する(ステップS20)。

【0047】したがって、この「出荷時情報記録処理」によれば、未記録のCD-R1のシステム領域にID情報、暗号鍵および作成日付などの隠し情報を書き込んで市場に出荷し、ユーザに届けられることができる。そして、ユーザ段階で、以下に説明するデータ書き込み処理、デ

14

ータ再生処理またはディスクコピー処理を行う際に、上記の隠し情報を利用した本実施の形態特有の処理を実行することができる。

【0048】<ユーザによるデータ書き込み処理>図8は、ユーザ段階で実行されるデータ書き込み動作(以下「ユーザによるデータ書き込み処理」という。)を示すフローチャートである。ユーザは上述の「出荷時情報記録処理」を終えたCD-R1を市場で入手し、そのCD-R1をCD-R記録再生装置10にセットして、図示の処理を開始する。

【0049】この処理を開始すると、まず、ホスト装置21からCD-R記録再生装置10へ書き込み命令が発行される。CD-R記録再生装置10はこの命令に responding CD-R1のシステム領域からID情報を読み出し(ステップS31)、サポートディスクであるか否かを判定する(ステップS32)。サポートディスクとは、前述のとおり、所定の製造者またはあらかじめ登録された製造者によって作られたディスクのことである。CD-R記録再生装置10はこれらの製造者を識別するためのID情報リスト(以下「サポートリスト」という。)を保持しており、上記のステップS32で当該サポートリストを参照してID情報が登録済みであれば、CD-R記録再生装置10にセットされているCD-R1がサポートディスクであると判定する。

【0050】ステップS32の判定結果が「否」(N)の場合、すなわち、CD-R記録再生装置10にセットされているCD-R1がサポートディスクでない場合は、ホスト装置21に対してサポートディスクへの交換を促す旨のメッセージ(例えば、「このディスクはセキュリティ対応ではありません。セキュリティ対応のディスクに交換してください。」)を送出(ステップS33)して、ディスク交換後の書き込み続行または書き込み中止を判定(ステップS38)する一方、ステップS32の判定結果が「肯」(YES)の場合、すなわち、CD-R記録再生装置10にセットされているCD-R1がサポートディスクである場合は、以下の処理を実行する。

【0051】まず、記録データに機密フラグを付加する(ステップS34)。この機密フラグは、前述のとおり、再生段階において、復号後の平文データの再利用を禁止するためのチェックフラグとして用いられるものであり、好ましくは、電子透かしのような技術を応用してその存在を秘匿化したデータのことである。次いで、CD-R記録再生装置10にセットされているCD-R1のシステム領域から暗号鍵を読み出し(ステップS36)、その暗号鍵を用いて上記の機密フラグを付加した記録データを暗号化した後、その暗号化データをCD-R1のユーザ領域に記録する(ステップS37)。

【0052】最後に、他のCD-R1に書き込みを行うか否かを判定し(ステップS38)、書き込みを継続す

(9)

特開2001-332019

15

る場合は、所要のメッセージ（例えば、「新しいディスクをセットしてください」）をホスト装置21に送出すると共に、書き込み済みのCD-R1をリジェクトしてステップS31以降を繰り返す、書き込みを継続しない場合は書き込み済みのCD-R1をリジェクトして処理を終了する。

【0053】図9は、上記「ユーザによるデータ書き込み処理」のタイムランを示す図である。この図において、ユーザは、CD-R1をCD-R記録再生装置10に装填すると共に、ホスト装置21を操作して所要の書き込み命令をCD-R記録再生装置10に発行する。CD-R記録再生装置10はこの書き込み命令にตอบสนองして、CD-R1のシステム領域に書き込まれたID情報を読み出し、所定のID情報リスト（サポートリスト）と照合してサポートディスクであるか否かを判定する。そして、サポートディスクでなければ、ホスト装置21に対してディスクの交換を促し、サポートディスクであれば、ホスト装置21に対してその旨を通知する。ホスト装置21はサポートディスクである旨の通知にตอบสนองして、記録データに機密フラグを付加し、CD-R記録再生装置10に対して暗号鍵を要求する。CD-R記録再生装置10はCD-R1のシステム領域から暗号鍵を読み出し、その暗号鍵をホスト装置21に転送する。ホスト装置21は転送された暗号鍵を用いて記録データ（機密フラグを付加したもの）を暗号化し、その暗号化データをCD-R記録再生装置10に転送し、CD-R記録再生装置10は転送された暗号化データをCD-R1に記録する。

【0054】したがって、この「ユーザによるデータ書き込み処理」によれば、所定のサポートリストに記載されたID情報を持つCD-R、要するに、特定の製造者によって作られたCD-Rについてのみ、そのユーザ領域に、機密フラグを付加した記録データを暗号化して記録することができるから、サポートリストに未記載の製造者によって作られたCD-Rとの差別化を図ることができる。

【0055】＜ユーザによるデータ再生処理＞図10は、ユーザ段階のデータ再生に用いられる再生専用機（以下「CD-R再生装置」という。）の概略的なブロック構成図であり、前述のCD-R記録再生装置10（図6参照）との相違は、データの記録機能を持たない点である。すなわち、このCD-R再生装置30（発明の要旨に記載のライトワンス型光ディスク用データ再生装置に相当）は、CD-R1のクランピングエリアを担持して所定方向に回転駆動するスピンドルモータ32と、CD-R1の基板1bを透して記録層1cに再生用のレーザ33を照射する光ピックアップ34と、光ピックアップ34の内部に設けられた不図示のシークモータと協調して光ピックアップ34をディスクの半径方向に移動させる粗動モータ35とを備えると共に、スピンドル

16

ルモータ32の回転速度を制御するディスク回転制御部36と、粗動モータ35の回転速度と回転方向を制御する粗動モータ制御部37と、光ピックアップ34の位置やレーザ強度の制御を行うピックアップ制御部38と、光ピックアップ34からの読み取り信号の波形変換等の制御を行う再生制御部39とを備え、さらに、これらの各制御部を統括するコントローラ40を備える。

【0056】このCD-R再生装置30は、前述のCD-R記録再生装置10と同様に、パーソナルコンピュータ等のホスト装置51の拡張スロットに内蔵され（または外付けされ）、ホスト装置51とコントローラ40との間を所定の信号規格（例えば、SCSI）のケーブル51aで接続して用いられる。

【0057】このような構成を有するCD-R再生装置30は、以下に示すとおり、CD-R1に書き込まれた情報の再生を行うことができる。なお、CD-R1はCD-ROMコンパチのデバイスであり、CD-R再生装置30は、先に説明したCD-R記録再生装置10と同様にCD-ROMの情報再生も可能であるが、本発明とは直接の関連がないため説明を省略する。

【0058】図11は、ホスト装置51の階層的機能概念図であり、図示の階層構造は、いわゆるOSI（Open System Interconnection：開放型システム間相互接続）参照モデルと同様に最下位層を物理層、最上位層をアプリケーション層とする構造を有している。この構造は大きく分けて、物理層と密接に関係するドライバ層51bと、その上位に位置するいわゆるオペレーティングシステム（OS）によって提供されるサービス層51cと、最上位層に位置してユーザインターフェースを実現するためのアプリケーション層51dとからなり、アプリケーション層51dに実装されたアプリケーションプログラム（例えば、CD-R再生装置30を利用するためのユーザインターフェースを含むもの）51eは、サービス層51cのオペレーティングシステム51fのAPI（Application Programmable Interface）を介してドライバ層51bにアクセスし、例えば、CD-R再生装置30をはじめとした各種リソースを利用する。

【0059】ここで、ドライバ層51bには多種多様なドライバプログラムが実装されている。例えば、CD-R再生装置30のインターフェース規格をSCSIとすると、少なくともSCSIドライバ（ATAPIドライバともいう）51gやSCSIポート用のミニポートドライバ51hおよび入出力制御用のIOS（Input/Output Supervisor）ドライバ51iなどが実装されている。

【0060】一般にアプリケーションプログラム51eはオペレーティングシステム51fの所定のAPIを利用して、物理層に位置する各種リソースを利用するが、通常、アプリケーションプログラム51eから見て、これらのドライバの存在は意識されない。例えば、アプリ

(10)

特開2001-332019

17

ケーションプログラム51eからCD-R再生装置30を利用する場合、実際には、I/Oドライブ51iやSCSIドライブ51gおよびミニポートドライブ51hを間接的に利用している。また、ファイルコピーの操作などを行う場合も、実際にはI/Oドライブ51iを間接的に利用している。

【0061】ところで、図示のドライブ層51bには、ハッチングで他と区別された特別なドライブ（以下「フィルタドライブ」という。）51jが実装されている。このフィルタドライブ51jは本実施形態に特有のもので、少なくとも（a）アプリケーションプログラム51eの要求に応じてCD-R再生装置30からオペレーティングシステム51fに渡されるデータをモニタし、そのデータ内に前述の「機密フラグ」が含まれているか否かを判定する第一の機能と、（b）上記「機密フラグ」の存在を判定した場合に当該データに対するオペレーティングシステム51fのコピー動作や保存動作を拒否しないしは制限（例えば、コピー命令や保存命令を無視したりすること）する第二の機能とを待つのであり、発明の要旨に記載の判定手段および禁止手段に相当するものである。

【0062】第一の機能を実現するために、フィルタドライブ51jはSCSIドライブ51gとミニポートドライブ51hの間に実装されており、さらに、第二の機能を実現するために、オペレーティングシステム51fとI/Oドライブ51iの間に実装されている。なお、この実装位置は一例である。要はアプリケーション層51dから直接的にアクセスできない位置であって、且つ、上記モニターと上記コピー動作や保存動作の拒否に適した位置に実装されていけばよい。また、フィルタドライブ51jは図示のように単一のものでなく、各機能ごとに分割されたものであってもよい。

【0063】ユーザは、アプリケーションプログラム51eによって提供されるユーザインターフェースを操作しながらCD-R再生装置30にアクセスし、CD-R1に記録されたデータの再生を行う。この再生処理に際して、オペレーティングシステム51fやドライブプログラム51g～51jは黒子的な仲介役となって表に出てこない。すなわち、ユーザは、オペレーティングシステム51fやドライブプログラム51g～51jの存在を意識することなく、CD-R再生装置30にアクセスし、CD-R1に記録されたデータを利用することができる。

【0064】CD-R1に記録されたデータは、アプリケーションプログラム51eから見て、オペレーティングシステム51cのファイルシステムによって管理された独立したデータの集まり（ファイル）として認識される。ユーザは、このデータを他の記憶デバイスに格納されたデータと同様に取り扱う（ファイルアクセス）ことができる。CD-R再生装置30は、このファイルアク

18

セスに際して、リードイン（RI）内のTOC情報を読み出してホスト装置51のドライブ層51bに提供すると共に、当該ドライブ層51bから特定ファイルの読み出しコマンドを受け取った場合は、リードイン（RI）内のTOC情報を参照して当該ファイルのデータが書き込まれたデータエリア（UA）のトラックを特定し、そのトラックの開始位置に光ピックアップ34を位置させると共に、スピンドルモータ32の回転速度を制御し、光ピックアップ34から再生用のレーザ33をCD-R1に照射して当該ファイルデータを読み取り、その読み取りデータをホスト装置51のドライブ層51bに転送するという一連の動作を実行する。

【0065】図12は、ユーザ段階で実行されるデータ再生動作（以下「ユーザによるデータ再生処理」という。）を示すフローチャートである。ユーザは、前述のユーザによるデータ書き込み処理によって暗号化データ（記録データに機密フラグを付加して暗号化したもの）が書き込まれたCD-R1を入手し、そのCD-R1をCD-R再生装置30にセットして、そのCD-R1からID情報を読み出す（ステップS41）と共に、ホスト装置51に対してID入力を要求する（ステップS42）。ホスト装置51は、画面上にID入力を促す旨の所定のGUI（Graphical User Interface）を表示してユーザによるキーボード等からのID入力を受け付け、入力されたID情報をCD-R記録再生装置10に転送する。CD-R再生装置30は、転送されたID情報とCD-R1から読み込んだID情報とを比較し（ステップS43）、一致した場合は正規ユーザ、一致しなかった場合は不正なユーザと判断し、不正ユーザの判断時にはそのまま処理を終了する一方、正規ユーザの判断時には、以下の処理を実行する。

【0066】まず、CD-R1のシステム領域に書き込まれている暗号鍵と暗号化データを読み出して（ステップS44、ステップS45）、ホスト装置51に転送する。ホスト装置51は、転送されたデータに機密フラグが含まれているか否かを判定し（ステップS46）、含まれている場合は、暗号鍵を用いてその暗号化データを復号し（ステップS47）、平文のデータに戻してユーザの利用に供する一方、機密フラグが含まれていない場合は、復号動作を行うことなく、そのまま処理を終了する。

【0067】図13は、上記「ユーザによるデータ再生処理」のタイムランを示す図である。この図において、ユーザは、CD-R1をCD-R再生装置30に装填すると共に、ホスト装置51を操作して所望の再生命令をCD-R再生装置30に発行する。CD-R再生装置30はこの再生命令にตอบสนองしてID要求をホスト装置51に返し、ホスト装置51は画面上にID入力を促す旨のGUIを表示する。ユーザは、そのGUIに従って所定のID情報（CD-R1の配布先から正当に通知された

(11)

特開2001-332019

19

ID情報)を入力し、ホスト装置51は入力されたID情報をCD-R再生装置30に転送する。

【0068】CD-R再生装置30は、CD-R1のシステム領域に書き込まれているID情報を読み出し、ホスト装置51から転送されたID情報との一致を判定して、不一致であれば不正ユーザと判断し、処理を中止して再生を拒否する一方、一致していれば正規ユーザと判断し、CD-R1のシステム領域に書き込まれている暗号鍵とデータエリアに書き込まれている暗号化データとを読み出してホスト装置51に転送する。ホスト装置51は、転送データ中に機密フラグがあるか否かを判定し、機密フラグが含まれている場合は、その暗号鍵を用いて暗号化データを復号し、正規ユーザからのアクセスを許容する一方、機密フラグが含まれていない場合は復号動作を行うことなく、処理を終了する。

【0069】したがって、この「ユーザによるデータ再生処理」によれば、CD-Rのシステム領域に書き込まれているID情報を用いて正規ユーザと不正ユーザとを識別することができ、正規ユーザによってデータ再生処理が行われている場合に、CD-Rのシステム領域に書き込まれた暗号鍵とデータエリアに書き込まれた暗号化データとをホスト装置に転送することができる。そして、転送データ中に機密フラグが含まれている場合に、ホスト装置で暗号化データの復号を行い、復号された生データへのアクセス（例えば、データの閲覧ないし実行等）を当該正規ユーザに許容することができる。

【0070】その結果、不正ユーザを排除してデータの再生を行うことができると共に、機密フラグが含まれている暗号化データの復号のみを行うことができるから、前記の「ユーザによるデータ書き込み処理」との組み合わせによって、記録段階から再生段階までの一連のセキュリティ対策を確立することができるうえ、このセキュリティ対策に欠くことのできない記録媒体として特定の製造者によって作られたサポートディスクの使用を強制することができる。

【0071】＜ユーザによるディスクコピー処理＞図14は、ユーザ段階で実行されるデータコピー動作（以下「ユーザによるデータコピー処理」という。）を示すフローチャートである。なお、以下の説明では、データのコピー先をCD-Rとしているが、これはデータ再利用の一例であり、コピー先は如何なる記憶媒体であってもよい。ハードディスクやその他の記録媒体であってもよい。

【0072】図14において、ユーザによるデータコピー処理を開始すると、ユーザは、前述のユーザによるデータ書き込み処理によって暗号化データ（記録データに機密フラグを付加して暗号化したもの）が書き込まれたCD-R1をコピー元、未記録のCD-Rをコピー先とし、それぞれをコピー元のCD-R再生装置30とコピー先のCD-R記録再生装置10にセットする。そして、

20

て、ホスト装置51を操作してコピー元のCD-R再生装置30にコピー命令を発行する。コピー元のCD-R再生装置30は、コピー命令にตอบสนองしてCD-R1からID情報を読み出す（ステップS51）と共に、ホスト装置51に対してID入力を要求する（ステップS52）。ホスト装置51は画面上にID入力を促す旨の所定のGUIを表示してユーザによるキーボード等からのID入力を受け付け、入力されたID情報をコピー元のCD-R再生装置30に転送する。

【0073】コピー元のCD-R再生装置30は、転送されたID情報とCD-R1から読み込んだID情報とを比較し（ステップS53）、一致した場合は正規ユーザ、一致しなかった場合は不正ユーザと判断し、不正ユーザの判断時にはそのまま処理を終了する一方、正規ユーザの判断時には、コピー元のCD-R1のシステム領域に書き込まれている暗号鍵と暗号化データを読み出してホスト装置51に転送する。ホスト装置51は、そのドライブ51bに実装されたフィルタドライブ51jにより、転送データ中に機密フラグが存在するか否かを判断し（ステップS54）、機密フラグが存在しなければ、転送された暗号鍵を用いて暗号化データを復号し、その復号データをコピー先のCD-R記録再生装置10に転送してコピー先のCD-R1に記録するというコピー処理を実行（ステップS55）して処理を終了する一方、機密フラグが存在していれば、同コピー処理を強制的に中止（ステップS56）して処理を終了する。

【0074】図15は、上記「ユーザによるデータコピー処理」のタイムランを示す図であり、図中のCD-R1とCD-R再生装置30はコピー元のもの、CD-R記録再生装置10とCD-R1'はコピー先のものである。この図において、ユーザは、コピー元とコピー先のCD-R1、1'をそれぞれCD-R再生装置30とCD-R記録再生装置10に装填すると共に、ホスト装置51を操作して所要のコピー命令をコピー元のCD-R再生装置30に発行する。コピー元のCD-R再生装置30はこのコピー命令にตอบสนองしてID要求をホスト装置51に返し、ホスト装置51は画面上にID入力を促す旨のGUIを表示する。ユーザは、そのGUIに従って所定のID情報（CD-R1の配布先から正当に通知されたID情報）を入力し、ホスト装置51は入力されたID情報をコピー元のCD-R再生装置30に転送する。

【0075】コピー元のCD-R再生装置30は、CD-R1のシステム領域に書き込まれているID情報を読み出し、ホスト装置51から転送されたID情報との一致を判定して、不一致であれば不正ユーザと判断し、処理を終了する一方、一致していれば正規ユーザと判断し、CD-R1に書き込まれている暗号鍵と暗号化データとを読み出してホスト装置51に転送する。ホスト装置51は、そのドライブ51bに実装されたフィルタ

(12)

特開2001-332019

21

ドライブ51」により、転送データ中の機密フラグの存在を判断する。そして、存在していればコピー処理を強制的に中止する一方、存在していなければ、暗号鍵を用いて暗号化データを復号し、その復号データをコピー先のCD-R記録再生装置10に転送し、コピー先のCD-R記録再生装置10はその転送データをCD-R1'に書き込む。

【0076】したがって、この「ユーザによるデータコピー処理」によれば、コピー元のCD-Rのシステム領域に書き込まれているID情報を用いて正規ユーザと不正ユーザとを識別することができると共に、機密フラグが付加されたデータのコピーが行われようとした場合は、たとえ正規ユーザであっても、そのコピー動作を強制的に中止（コピー動作の拒否）して実行しないようにすることができる。その結果、暗号化データに機密フラグが存在する場合は、コピー処理を積極的に禁止できるから、復号データの再利用を阻止することができ、記録から再生までのすべての段階にわたってセキュリティを保持させることができる。

【0077】<まとめ>以上、説明したとおり、本実施の形態によれば、CD-R1のシステム領域に書き込まれたID情報を用いて、サポートリストに記載された製造者のCD-R1（サポートディスク）であるか否かを判定でき、サポートディスクの場合に所定の機密フラグを付加した記録データを暗号化してCD-R1に記録することができる。そして、再生側でこの暗号化データを読み出す際に、機密フラグの有無を検査し、機密フラグがある場合に復号データの再利用を禁止することができる。したがって、ホスト装置51の内部には、前述の「ユーザによるデータ再生処理」によってメインメモリ上に一時的に作られた復号データしか存在しないため、しかも、この一時的データはプロセスからの利用完了時点で速やかに解放されるため、再利用可能な復号データの痕跡が残されることはなく、データの不正流出等を確実に防止することができるという格別有益な効果が得られる。

【0078】なお、以上の説明では、ID情報や暗号鍵などの隠し情報をシステム領域に書き込んでいるが、このシステム領域とは、ユーザによる直接的なアクセスが許容された領域（典型的にはデータエリア）以外の領域という意味であり、前述のPCAやPMAはもちろんのこと、リードインであってもよいし、リードアウトであってもよく、あるいは、これ以外の領域が存在するならば、その領域であってもよい。

【0079】また、暗号鍵については、特に説明を加えなかったが、一般的に知られている様々な暗号化方式（例えば、前述のDES方式以外にも、FEAL: Fast Encipherment Algorithmなどの方式がある。）のいずれを採用してもかまわない。解読の困難性、暗号化処理や復号処理のオーバーヘッドおよび暗号化データのポリュ

22

ーム等を勘案して適切な方式を採用すればよい。

【0080】また、前記説明のセキュリティ機能のうち、特に復号データの再利用を禁止する機能は、もっぱらホスト装置51に実装されたフィルタドライブ51jやその他の汎用ドライブおよびオペレーティングシステム等のソフトウェアリソースと、ホスト装置51の各種ハードウェアリソースとの有機的結合によって機能的に実現されるものであるが、フィルタドライブ51j以外のリソースは汎用のものを利用できるから、前記説明の「復号データの再利用を禁止する機能」として欠くことのできない必須の事項は、實質的に、フィルタドライブ51jのプログラムに集約されているということがいえる。したがって、本発明に係るセキュリティ機能のポイントは、それらのプログラムのすべてまたはその要部を格納した、フロッピーディスク、光ディスク、コンパクトディスク、磁気テープ、ハードディスクまたは半導体メモリなどの記録媒体若しくはこれらの記録媒体を含む備成品（ユニット品や完成品または半完成品）を包含する。なお、その記録媒体または備成品は、それ自体が流通経路にのるものはもちろんのこと、ネットワーク上にあって記録内容だけを提供するものも含まれる。

【0081】また、以上の説明では、ライトワンス型光ディスクとしてCD-Rの例を示したが、これに限らない。例えば、DVD（Digital Video DiscまたはDigital Versatile Disc）-Rも1回だけのデータ書き込みを行うことができるから、もちろんライトワンス型光ディスクの仲間である。上記説明をDVD-Rに適用する場合、CD-RをDVD-Rと読み替えると共に、CD-R記録再生装置やCD-RライターをそれぞれDVD-R記録再生装置、DVD-Rライターと読み替ればよい。

【0082】

【発明の効果】請求項1記載の発明によれば、データの再生時に所定の機密フラグが検出されると、再生データの複製物の生成が制限される。したがって、再生データの再利用を阻止して、再生段階におけるセキュリティを確保することができる。請求項2記載の発明によれば、光ディスクのシステム領域に不可視状態で格納されたセキュリティ情報に基づいて光ディスクへのアクセスが制限される。したがって、例えば、データ再生時に正当なユーザを認証して書き込みデータへのアクセスを許容することができ、不正ユーザの排除等、セキュリティ性の向上を図ることができる。請求項3記載の発明によれば、データの再生時に所定の機密フラグが検出されると、再生データの複製物の生成が禁止される。したがって、再生データの再利用を阻止して、再生段階におけるセキュリティを確保することができる。請求項4記載の発明によれば、マイクロコンピュータを含むハードウェアリソースと該プログラムとの有機的結合によって前記判定手段および禁止手段を実現できる。

(13)

特開2001-332019

23

24

【図面の簡単な説明】

【図1】本実施形態のCD-Rの利用模式図である。

【図2】ライトワンス型光ディスクの外観図およびその要部拡大図である。

【図3】CD-Rの断面構造図である。

【図4】CD-Rの各記録領域のフォーマット概念図である。

【図5】CD-Rのシステム領域に書き込まれるID情報と暗号鍵を含むデータフォーマットの例示構造図である。

【図6】CD-R記録再生装置の概略的なブロック構成図である。

【図7】出荷時情報記録処理を示すフローチャートである。

【図8】ユーザによるデータ書き込み処理を示すフローチャートである。

【図9】ユーザによるデータ書き込み処理のタイムランを示す図である。

*【図10】CD-R再生装置の概略的なブロック構成図である。

【図11】ホスト装置の階層的機能概念図である。

【図12】ユーザによるデータ再生処理を示すフローチャートである。

【図13】ユーザによるデータ再生処理のタイムランを示す図である。

【図14】ユーザによるディスクコピー処理を示すフローチャートである。

10 【図15】ユーザによるディスクコピー処理のタイムランを示す図である。

【図16】従来のセキュリティ対策の概念図である。

【符号の説明】

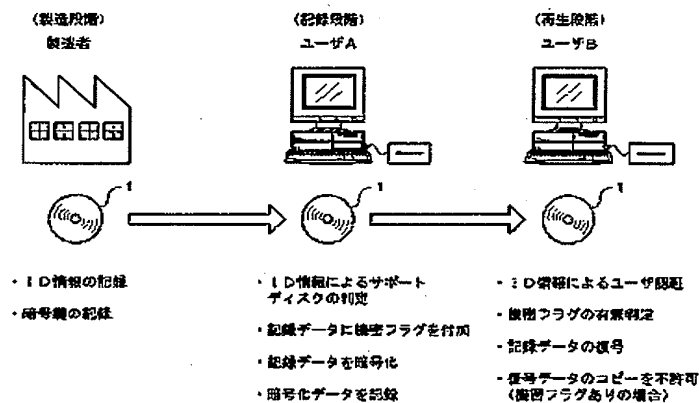
PCA Power Calibration Area (システム領域)

1 CD-R (ライトワンス型光ディスク)

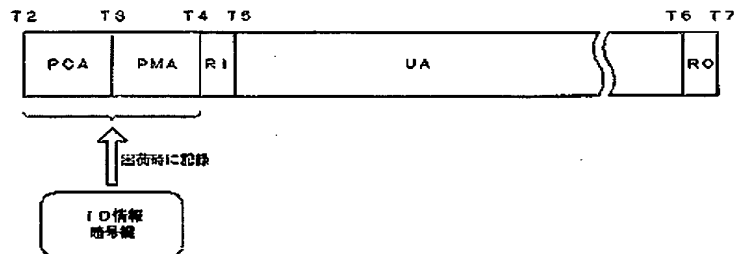
30 CD-R再生装置 (ライトワンス型光ディスク用データ再生装置)

* 51 1 フィルタドライバ (判定手段、禁止手段)

【図1】



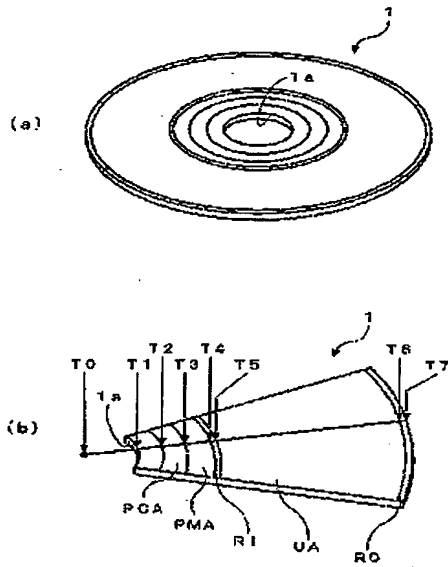
【図4】



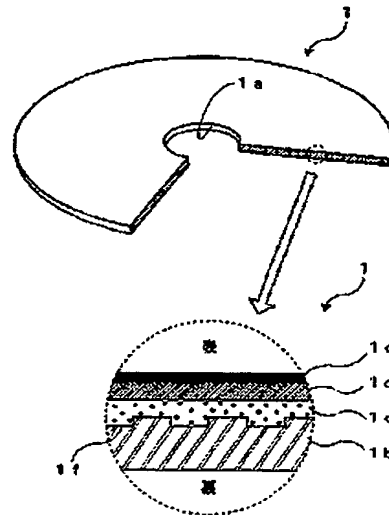
(14)

特開2001-332019

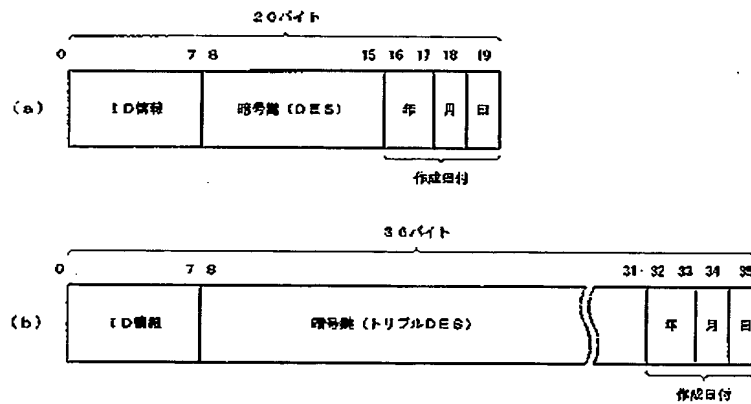
【図2】



【図3】



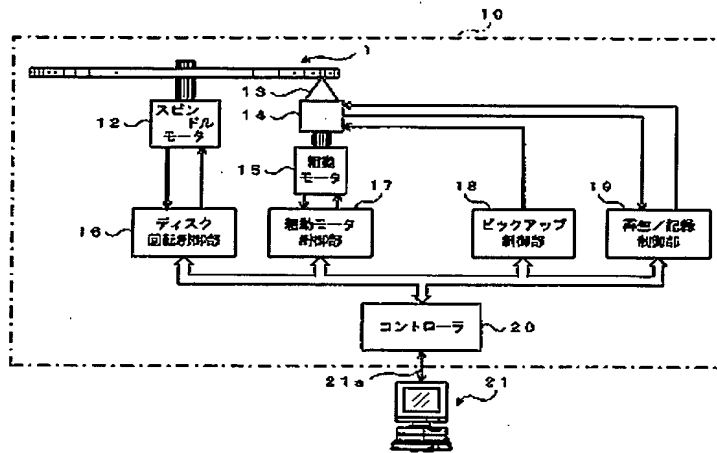
【図5】



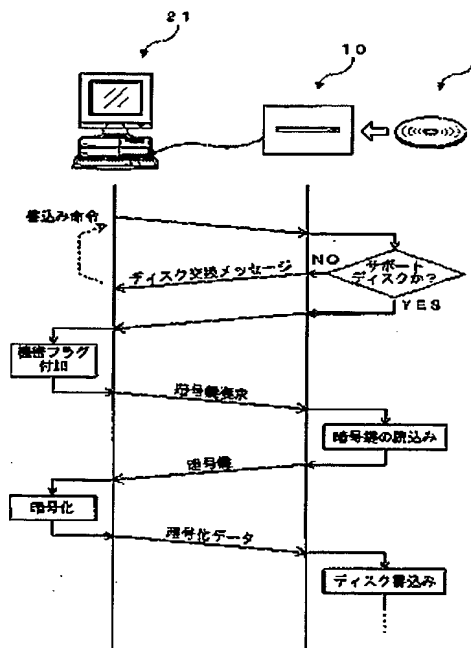
(15)

特開2001-332019

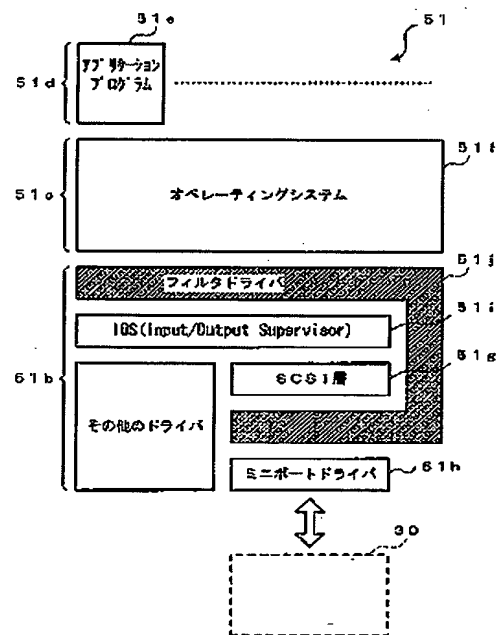
【図6】



【図9】



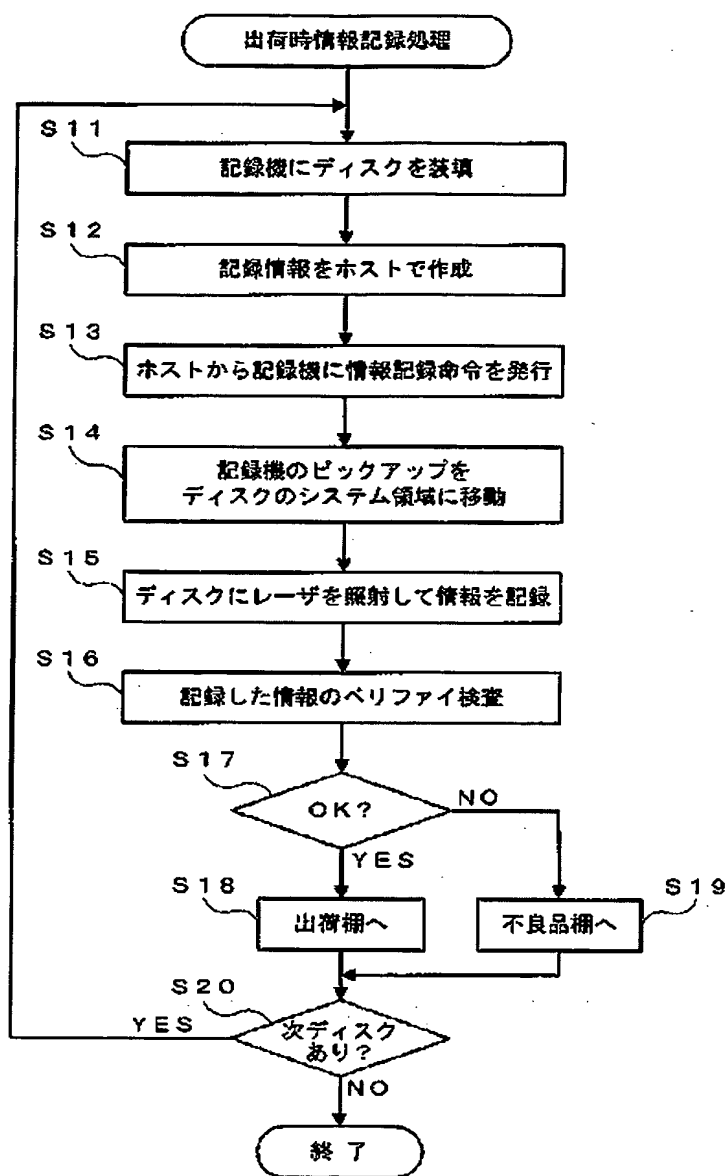
【図11】



(15)

特開2001-332019

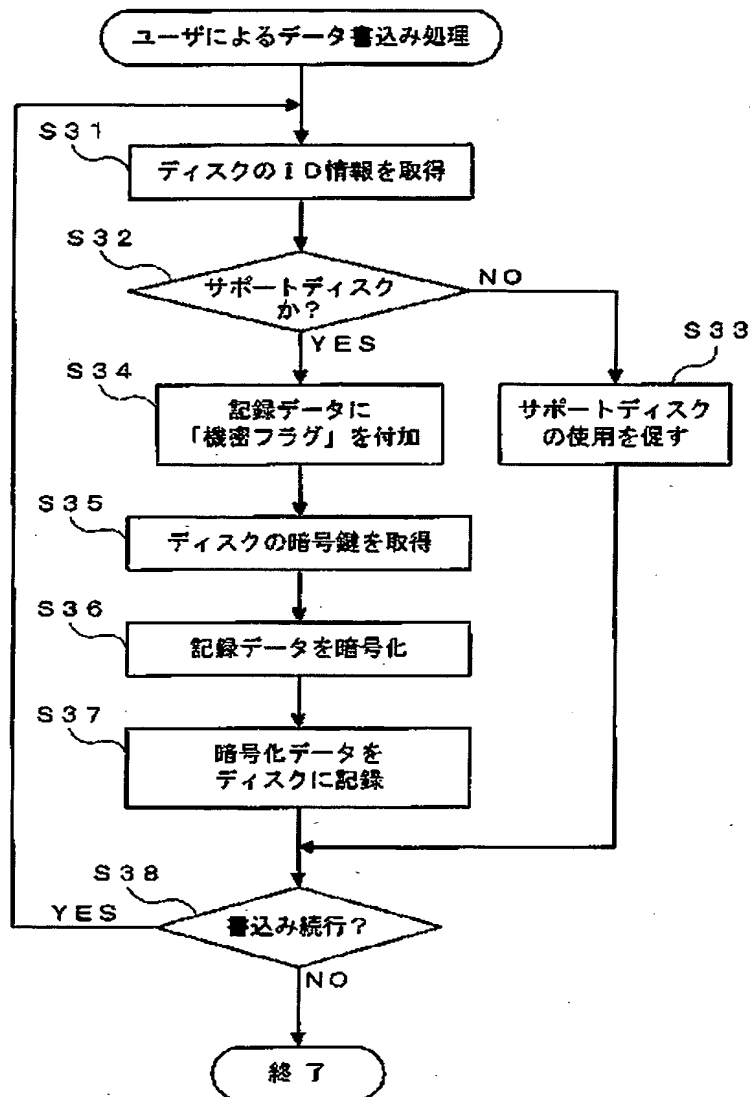
【図7】



(17)

特開2001-332019

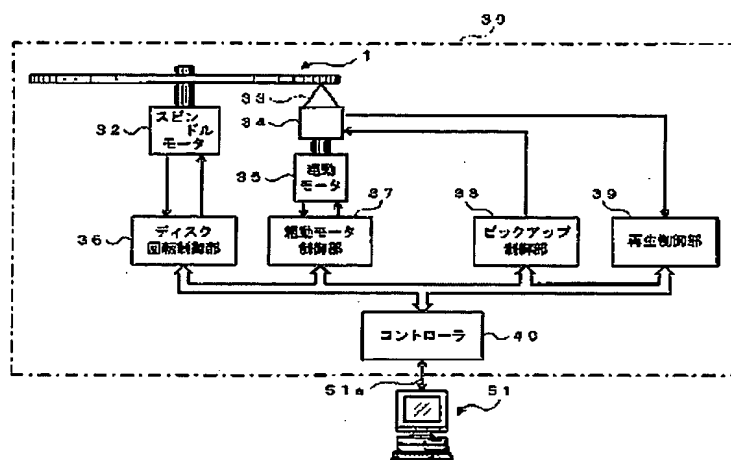
【図8】



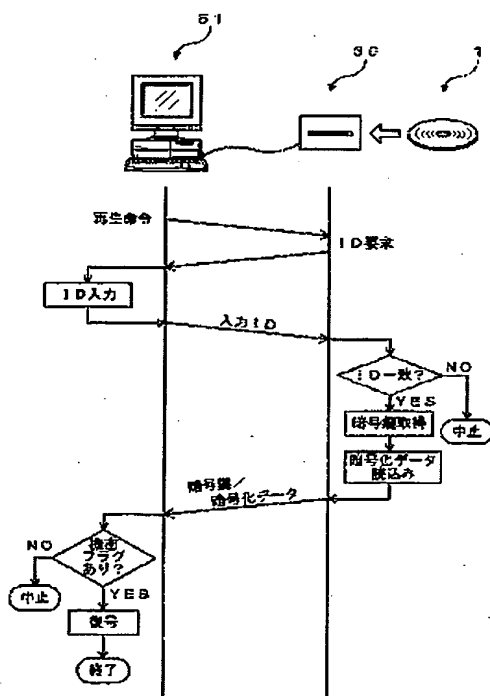
(18)

特開2001-332019

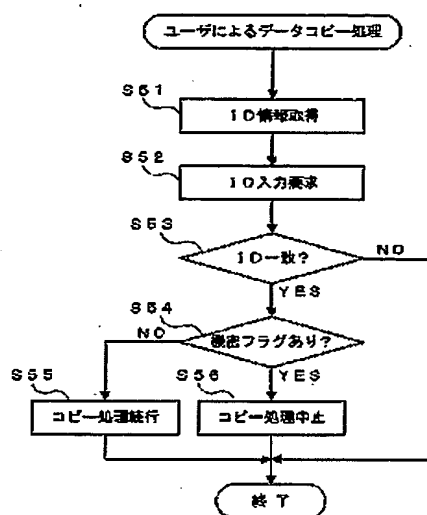
【図10】



【図13】



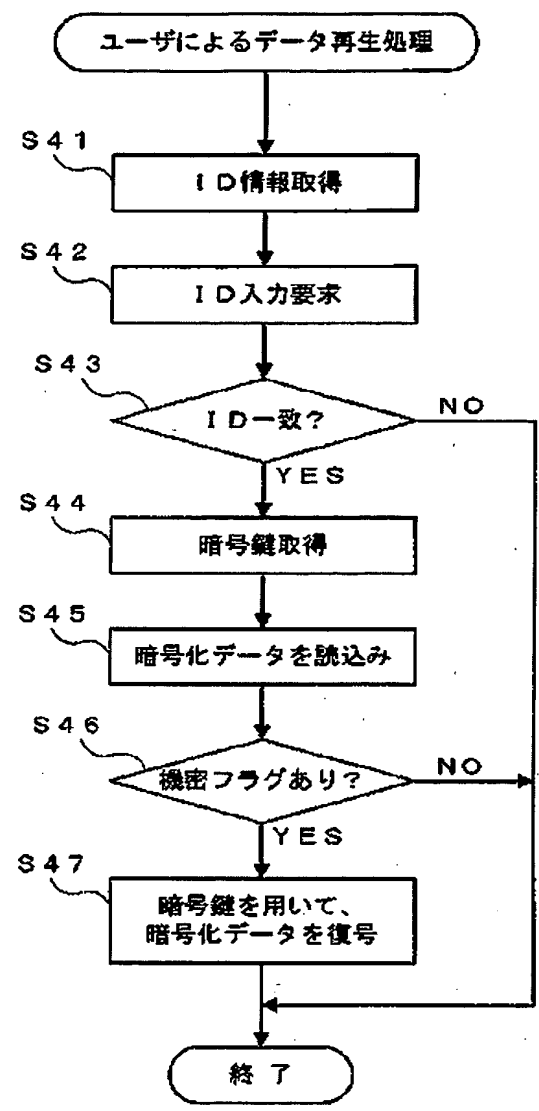
【図14】



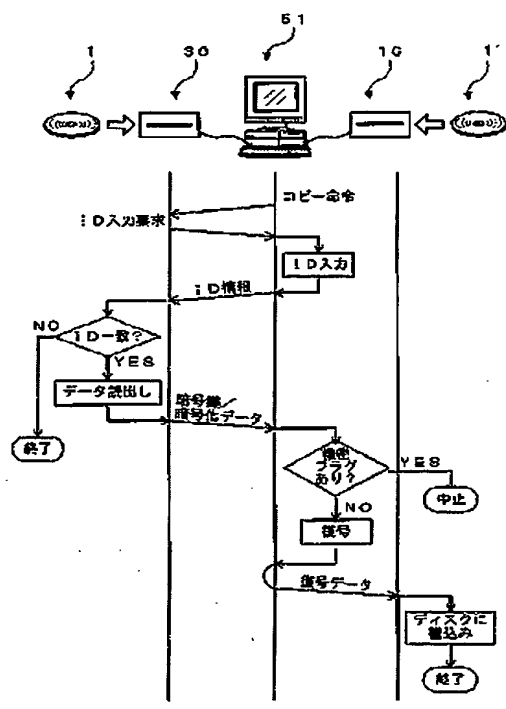
(19)

特開2001-332019

【図12】



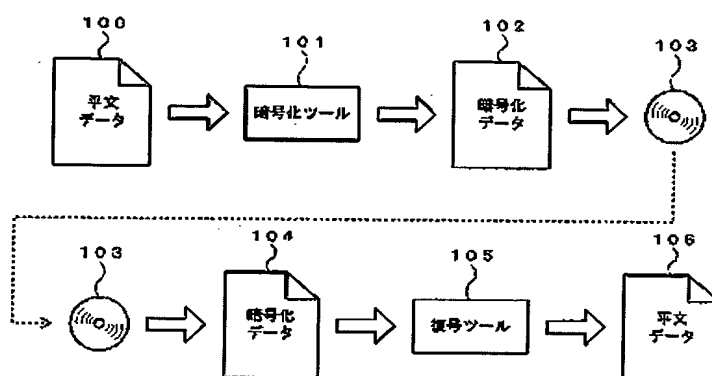
【図15】



(20)

特開2001-332019

【図16】



 フロントページの続き

(72)発明者 清水 洋信
 東京都台東区上野6丁目16番20号 太陽誘
 電株式会社内

Fターム(参考) 5D044 BC05 CC04 DE17 DE50 EF05
 FG18 GK12 HL08

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.